WEST

Generate Collection

L1: Entry 3 of 5 File: USPT Mar 30, 1993

DOCUMENT-IDENTIFIER: US 5199070 A
TITLE: Method for generating a public key

BSPL:
Note that (mod q) represents an equation in which the residue is determined by dividing by q. Given S, q and g in equation [1], P is easily calculated. If P, q, and g are known, however, determining S becomes more and more difficult as q increases. S is called a discrete logarithm of P wherein q is its modulus and g is its base. Determining S is well known as the discrete logarithm problem.

DEPR:
In any of the embodiments 1 through 4, g is a primitive root of the residue-class field with q as modulus. The primitive root g is a positive integer equal to or less than (q-1), with q assumed to be a prime number, and the primitive root g to (q-1)st power is 1 in connection with mod q (g.sup.q-1 =1 mod q). Alternatively, an integer g' may replace g, by using a divisor q' of (q-1); thus, g' to q' power is 1 in connection with mod q (g.sup.q' =1 mod q, q': the divisor of q-1). This is fully discussed in the paper authored by C. P. Schnorr, entitled "Efficient Identification and Signatures For Smart Cards" in Proc. CRYPT089. Although the use of g' provides less security against an exhaustive attach to cope with the discrete logarithm problem, compared with the case where the primitive root g is used, the workload involved in calculations on the users is alleviated. For example, calculation process amount of the public key generation step in the first embodiment is approx. (1.5.times.log .sub.2 q'+0.25.times.log .sub.2 Hi) times of residue of the multiplication calculation process per log .sub.2 q bit width on average. To assure sufficient security, in this case, a value of 140 bits or larger may be used for q'. Substituting 140 for log .sub.2 q', and 128 for log .sub.2 Hi, results in 242 as the number of iteration in calculation. Therefore, it is almost three times as fast as the first embodiment.

WEST

Generate Collection

L1: Entry 4 of 5 File: TDBD Nov 1, 1990

DOCUMENT-IDENTIFIER: NB9011166
TITLE: Fast Division Using Table Look-Up.

TBTX:
- Described is a method of converting a 'Logical Block Address' to cylinder track and sector values on a microprocessor without a divide instruction. After breaking the dividend into bytes, look-up tables are used to find quotients and remainders. Carries are used while computing the remainder to adjust the quotient. Speed is gained at the expense of table space. - Microprocessors which do not have a built-in divide instruction need software algorithms to perform division. These are usually implemented as a loop, containing subtraction and shifting operations, executed as many times as there are bits in the dividend and, in consequence, are slow. When the divisor is a known constant and if execution time is critical, a faster algorithm is required. - An example is when dividing a logical block address (LBA) received in a SCSI command by the number of sectors per cylinder, to get the cylinder address. The remainder of the division is then further divided by the number of heads, to get the track and sector numbers. - The advantages of this algorithm are fast execution with both quotient and remainder generated. When dividing an N-byte number (the dividend) by a given constant divisor (K), the dividend is first split up into N parts, at byte boundaries. - Example: (N=3) '123456'x = '120000'x + '3400'x + '56'x i2='12'x i1='34'x i0='56'x Each index i is then used as an index into a table of 256 entries which gives both the quotient and remainder when that part of the dividend is divided by divisor K. - Thus, i2 in the example is used as an index into Table2 which contains entries: i2 quotient remainder 0 '00000'x DIV K '00000'x MOD k 1 '10000'x DIV K '10000'x MOD k 2 '20000'x DIV K '20000'x MOD k : : : : : : 255 'FF0000'x DIV K 'FF0000'x MOD k Similar tables Table1 and Table0 are used with i1 and i0. - This results in N quotient values and N remainder values being extracted from the tables; quotient values are summed to give a total Q. The remainder values are then also added, giving R, with a test after each addition for whether the sum exceeds the divisor K. If it does, K is subtracted and Q is incremented by 1. There are N-1 addition operations to generate R. The result is the quotient Q and remainder R. - A few short-cuts may be applied to reduce the amount of storage occupied by the tables. If the divisor exceeds '100'x, then the remainders in Table0 will be equal to the index i0, and so the 'remainder' half of Table0 is unnecessary. If the divisor exceeds '10000'x, then this applies to Table1 also, etc. Should the range of dividend values be restricted, then not all of the most-significant table is required. For example, with N=3, if the dividend never exceeds '1FFFFF'x, then Table2 need only have the first '20'x entries.

WEST

Generate Collection

L1: Entry 1 of 5 File: USPT Aug 14, 2001

DOCUMENT-IDENTIFIER: US 6275311 B1
TITLE: Optical device for processing an optical digital signal

DEPR:
So far, the decoding algorithm has been implemented by electronic digital hardware based on serial data processing (U.S. Pat. No. 5,402,429; Maniatopoulos A. et al., "Single-bit error-correction circuit for ATM interfaces", Electronics Letters, 31, No. 8, 617-618, 1995; Maniatopoulos A. et al., "Implementation issues of the ATM cell delineation mechanism", Electronics Letters, 32, No. 11, 963-965, 1996). The decoder is usually a simple dedicated DSP circuit employing a serial shift register as fundamental device, essentially able to perform a binary polynomial division. The scheme of such circuit is well known (FIG. 13). To divide two polynomials the shift register must have a number of flip-flop cells equal to the degree of the divisor, and a pattern of logic "feedback loops" configured according to the coefficients of the divisor. Each feedback loop feeds bits from the last stage of the shift register to a summing node (modulo-2 sum, or XOR). Into the summing nodes the back fed bits are added to the output of an intermediate flip-flop. Before starting the operation, all flip-flops must be cleared. The dividend bits flow sequentially into the first flip-flop starting from the most significant, and at each clock pulse they are shifted one step towards the last cell. When the last dividend bit has entered the device the division remainder bits are kept stored into the memory cells of the shift register. They can be read from the output by shifting again, after all the feedback loops have been opened.

WEST

Generate Collection

L10: Entry 2 of 14 File: USPT Sep 26, 2000

DOCUMENT-IDENTIFIER: US 6125380 A
TITLE: Dividing method

BSPR:
The shift-dividing have following steps. At first an initital value is set for a counting value. Secondly, the high-byte remainder is leftwardly shifted one bit to obtain a number. Then, the divisor is substracted from the number to update the high-byte remainder and the counting value is added to the low-byte quotient to update the high-byte quotient when the number is not less than the divisor. The counter is circularly and rightwardly shifting one bit. Finally, the step that the high-byte remainder is leftwardly shifted one bit is repeated until the counting value returns to the initital value.

WEST

Help | Logout | Interrupt

Main Menu | Search Form | Posting Counts | Show S Numbers | Edit S Numbers | Preferences

Search Results -

Term	Documents
MODULO.DWPI,TDBD,EPAB,JPAB,USPT,PGPB.	16147
MODULOES.DWPI,TDBD,EPAB,JPAB,USPT,PGPB.	1
MODULOS.DWPI,TDBD,EPAB,JPAB,USPT,PGPB.	70
MODULOE.DWPI,TDBD,EPAB,JPAB,USPT,PGPB.	1
MODULI.DWPI,TDBD,EPAB,JPAB,USPT,PGPB.	7221
MODULIS.DWPI,TDBD,EPAB,JPAB,USPT,PGPB.	24
MOD.DWPI,TDBD,EPAB,JPAB,USPT,PGPB.	15280
MODS.DWPI,TDBD,EPAB,JPAB,USPT,PGPB.	305
MODULUS.DWPI,TDBD,EPAB,JPAB,USPT,PGPB.	114339
MODULU.DWPI,TDBD,EPAB,JPAB,USPT,PGPB.	34
(L7 AND (MODULO OR MODULI OR MOD OR MODULUS)SAME(REMAINDER OR RESIDU$3) SAME DIVI$7 SAME (ITERAT$8 OR LOOP$4 OR BRANCH$4 OR RECUR$7) SAME REED$1SOLOMON).USPT,PGPB,JPAB,EPAB,DWPI,TDBD.	0

There are more results than shown above. Click here to view the entire set.

Database:
US Patents Full-Text Database
US Pre-Grant Publication Full-Text Database
JPO Abstracts Database
EPO Abstracts Database
Derwent World Patents Index
IBM Technical Disclosure Bulletins

Refine Search: 17 and (modulo or moduli or mod or modulus)same(remainder or residu$3) same divi$7 same | Clear

Search History

Today's Date: 9/25/2001

DB Name	Query	Hit Count	Set Nam
USPT,PGPB,JPAB,EPAB,DWPI,TDBD	l7 and (modulo or moduli or mod or modulus)same(remainder or residu$3) same divi$7 same (iterat$8 or loop$4 or branch$4 or recur$7) same reed$1solomon	0	L8
USPT,PGPB,JPAB,EPAB,DWPI,TDBD	(modulo or moduli or mod or modulus)same(remainder or residu$3) same divi$7 same (iterat$8 or loop$4 or branch$4 or recur$7)	74	L7
USPT,PGPB,JPAB,EPAB,DWPI,TDBD	l5 and (modulo or moduli or mod or modulus)same(remain$4 or residu$3) same divi$7 same (iterat$8 or loop$4 or branch$4 or recur$7)	104	L6
USPT,PGPB,JPAB,EPAB,DWPI,TDBD	(remain$4 or residu$3) same divi$7 same (iterat$8 or loop$4 or branch$4 or recur$7)	4475	L5
USPT,PGPB,JPAB,EPAB,DWPI,TDBD	(modulo or moduli or mod or modulus)same (remain$4 or residu$3) same divi$7 same (iterat$8 or loop$4 or branch$4 or recur$7) same (bit or binary or digit$4) same (divisor or dividend)	5	L4
USPT,PGPB,JPAB,EPAB,DWPI,TDBD	('NB9011166')[ABPN1,NRPN,PN,TBAN,WKU]	1	L3
USPT,PGPB,JPAB,EPAB,DWPI,TDBD	('5199070'| 'NB9011166'| '5928315'| '6275311'| 'NN72053726')[ABPN1,NRPN,PN,TBAN,WKU]	9	L2
USPT,PGPB,JPAB,EPAB,DWPI,TDBD	(((((modulo or moduli or mod or modulus)same (remain$4 or residu$3) same divi$7)and (modulo or moduli or mod or modulus)same (remain$4 or residu$3) same divi$7 same (iterat$8 or loop$4 or branch$4))and (modulo or moduli or mod or modulus)same (remain$4 or residu$3) same divi$7 same (iterat$8 or loop$4 or branch$4) same (bit or binary or digit$4)) and (modulo or moduli or mod or modulus)same (remain$4 or residu$3) same divi$7 same (iterat$8 or loop$4 or branch$4) same (bit or binary or digit$4) same (divisor or dividend))	5	L1

WEST

Freeform Search

Database:
US Patents Full-Text Database
US Pre-Grant Publication Full-Text Database
JPO Abstracts Database
EPO Abstracts Database
Derwent World Patents Index
IBM Technical Disclosure Bulletins

Term: 14 and (modulo or moduli or mod or modulus)same (remain$4 or residu$3) same divi$7 same (iterat$8 or loop$4 or branch$4) same (bit or binary or digit$4) same (divisor or dividend)

Display: 20 **Documents in Display Format:** CIT **Starting with Number** 1

Generate: ○ Hit List ◉ Hit Count ○ Image

Search | Clear | Help | Logout | Interrupt

Main Menu | Show S Numbers | Edit S Numbers | Preferences

Search History

Today's Date: 9/25/2001

DB Name	Query	Hit Count	S Na
USPT,PGPB,JPAB,EPAB,DWPI,TDBD	('6275311'| '5199070'| 'NB9011166'| '5928315'| 'NN72053726')[ABPN1,NRPN,PN,TBAN,WKU]	9	L
USPT,PGPB,JPAB,EPAB,DWPI,TDBD	l4 and (modulo or moduli or mod or modulus)same (remain$4 or residu$3) same divi$7 same (iterat$8 or loop$4 or branch$4) same (bit or binary or digit$4) same (divisor or dividend)	5	L
USPT,PGPB,JPAB,EPAB,DWPI,TDBD	l2 and (modulo or moduli or mod or modulus)same (remain$4 or residu$3) same divi$7 same (iterat$8 or loop$4 or branch$4) same (bit or binary or digit$4)	31	L
USPT,PGPB,JPAB,EPAB,DWPI,TDBD	('6275311')[ABPN1,NRPN,PN,TBAN,WKU]	2	L
USPT,PGPB,JPAB,EPAB,DWPI,TDBD	l1 and (modulo or moduli or mod or modulus)same (remain$4 or residu$3) same divi$7 same (iterat$8 or loop$4 or branch$4)	97	L
USPT,PGPB,JPAB,EPAB,DWPI,TDBD	(modulo or moduli or mod or modulus)same (remain$4 or residu$3) same divi$7	1718	L

WEST

Help Logout Interrupt

Main Menu | Search Form | Posting Counts | Show S Numbers | Edit S Numbers | Preferences

Your wildcard search against 2000 terms has yielded the results below

Search for additional matches among the next 2000 terms

Search Results -

Term	Documents
MODULO.DWPI,TDBD,EPAB,JPAB,USPT,PGPB.	16147
MODULOES.DWPI,TDBD,EPAB,JPAB,USPT,PGPB.	1
MODULOS.DWPI,TDBD,EPAB,JPAB,USPT,PGPB.	70
MODULOE.DWPI,TDBD,EPAB,JPAB,USPT,PGPB.	1
MODULI.DWPI,TDBD,EPAB,JPAB,USPT,PGPB.	7221
MODULIS.DWPI,TDBD,EPAB,JPAB,USPT,PGPB.	24
MOD.DWPI,TDBD,EPAB,JPAB,USPT,PGPB.	15280
MODS.DWPI,TDBD,EPAB,JPAB,USPT,PGPB.	305
MODULUS.DWPI,TDBD,EPAB,JPAB,USPT,PGPB.	114339
MODULU.DWPI,TDBD,EPAB,JPAB,USPT,PGPB.	34
. . . . .	
SUM$7(SUMMATING).USPT,PGPB,JPAB,EPAB,DWPI,TDBD.	pickup term
(L10 AND (MODULO OR MODULI OR MOD OR MODULUS)SAME (REMAINDER OR RESIDU$3) SAME DIVI$7 SAME(COMBIN$6 OR ADD$8 OR SUM$7 OR SUB$1TRACT$3)NEAR (LOW$3 OR UP$3)NEAR (BIT OR NUMBER OR DIGIT OR VALUE)).USPT,PGPB,JPAB,EPAB,DWPI,TDBD.	0

There are more results than shown above. Click here to view the entire set.

Database:
US Patents Full-Text Database
US Pre-Grant Publication Full-Text Database
JPO Abstracts Database
EPO Abstracts Database
Derwent World Patents Index
IBM Technical Disclosure Bulletins

Refine Search:
l10 and (modulo or moduli or mod or modulus)same (remainder or residu$3) same divi$7 same(combin$6 or add$8 or

Clear

Search History

Today's Date: 9/25/2001

DB Name	Query	Hit Count	S Na
USPT,PGPB,JPAB,EPAB,DWPI,TDBD	l10 and (modulo or moduli or mod or modulus)same (remainder or residu$3) same divi$7 same(combin$6 or add$8 or sum$7 or sub$1tract$3)near (low$3 or up$3)near (bit or number or digit or value)	0	L
USPT,PGPB,JPAB,EPAB,DWPI,TDBD	('5867412')[ABPN1,NRPN,PN,TBAN,WKU]	3	L
USPT,PGPB,JPAB,EPAB,DWPI,TDBD	l9 and (remainder or residu$3) same divi$7 same(combin$6 or add$8 or sum$7 or sub$1tract$3)near (low$3 or up$3)near (bit or number or digit or value)	14	L
USPT,PGPB,JPAB,EPAB,DWPI,TDBD	(combin$6 or add$8 or sum$7 or sub$1tract$3)near (low$3 or up$3)near (bit or number or digit or value)	1823	L
USPT,PGPB,JPAB,EPAB,DWPI,TDBD	l7 and (modulo or moduli or mod or modulus)same(remainder or residu$3) same divi$7 same (iterat$8 or loop$4 or branch$4 or recur$7) same reed$1solomon	0	L
USPT,PGPB,JPAB,EPAB,DWPI,TDBD	(modulo or moduli or mod or modulus)same(remainder or residu$3) same divi$7 same (iterat$8 or loop$4 or branch$4 or recur$7)	74	L
USPT,PGPB,JPAB,EPAB,DWPI,TDBD	l5 and (modulo or moduli or mod or modulus)same(remain$4 or residu$3) same divi$7 same (iterat$8 or loop$4 or branch$4 or recur$7)	104	L
USPT,PGPB,JPAB,EPAB,DWPI,TDBD	(remain$4 or residu$3) same divi$7 same (iterat$8 or loop$4 or branch$4 or recur$7)	4475	L
USPT,PGPB,JPAB,EPAB,DWPI,TDBD	(modulo or moduli or mod or modulus)same (remain$4 or residu$3) same divi$7 same (iterat$8 or loop$4 or branch$4 or recur$7) same (bit or binary or digit$4) same (divisor or dividend)	5	L
USPT,PGPB,JPAB,EPAB,DWPI,TDBD	('NB9011166')[ABPN1,NRPN,PN,TBAN,WKU]	1	L
USPT,PGPB,JPAB,EPAB,DWPI,TDBD	('5199070'| 'NB9011166'| '5928315'| '6275311'| 'NN72053726')[ABPN1,NRPN,PN,TBAN,WKU]	9	L
	(((((modulo or moduli or mod or modulus)same (remain$4 or residu$3) same divi$7)and (modulo or moduli or mod or modulus)same (remain$4 or residu$3) same divi$7 same (iterat$8 or loop$4 or		

USPT,PGPB,JPAB,EPAB,DWPI,TDBD	branch$4))and (modulo or moduli or mod or modulus)same (remain$4 or residu$3) same divi$7 same (iterat$8 or loop$4 or branch$4) same (bit or binary or digit$4)) and (modulo or moduli or mod or modulus)same (remain$4 or residu$3) same divi$7 same (iterat$8 or loop$4 or branch$4) same (bit or binary or digit$4) same (divisor or dividend))	5	L

WEST

Search Results - Record(s) 1 through 20 of 34 returned.

L13: Entry 1 of 34 File: USPT Nov 14, 2000

US-PAT-NO: 6148203
DOCUMENT-IDENTIFIER: US 6148203 A

TITLE: Method for registering a communication device for communication service
DATE-ISSUED: November 14, 2000

US-CL-CURRENT: 455/434; 455/166.1, 455/435, 455/62

INT-CL: [7] H04Q 7/20

L13: Entry 2 of 34 File: USPT Sep 26, 2000

US-PAT-NO: 6125380
DOCUMENT-IDENTIFIER: US 6125380 A

TITLE: Dividing method
DATE-ISSUED: September 26, 2000

US-CL-CURRENT: 708/650; 708/653

INT-CL: [7] G06F 7/52

L13: Entry 3 of 34 File: USPT Feb 2, 1999

US-PAT-NO: 5867412
DOCUMENT-IDENTIFIER: US 5867412 A

TITLE: Modular multiplication device for information security
DATE-ISSUED: February 2, 1999

US-CL-CURRENT: 708/491; 380/28, 708/620

INT-CL: [6] G06F 7/38

L13: Entry 4 of 34 File: USPT Feb 3, 1998

US-PAT-NO: 5715376
DOCUMENT-IDENTIFIER: US 5715376 A

TITLE: Data transformation apparatus
DATE-ISSUED: February 3, 1998

US-CL-CURRENT: 358/1.9; 358/523, 358/525

INT-CL: [6] H04N 1/56

L13: Entry 5 of 34 File: USPT Apr 8, 1997

US-PAT-NO: 5619440
DOCUMENT-IDENTIFIER: US 5619440 A

TITLE: Multiplier circuit with rounding-off function
DATE-ISSUED: April 8, 1997

US-CL-CURRENT: 708/620; 708/551

INT-CL: [6] G06F 7/52

L13: Entry 6 of 34 File: USPT Aug 22, 1995

US-PAT-NO: 5444647
DOCUMENT-IDENTIFIER: US 5444647 A

TITLE: Multiplier circuit and division circuit with a round-off function
DATE-ISSUED: August 22, 1995

US-CL-CURRENT: 708/650

INT-CL: [6] G06F 7/52

L13: Entry 7 of 34 File: USPT May 10, 1994

US-PAT-NO: 5311192
DOCUMENT-IDENTIFIER: US 5311192 A

TITLE: Polarization ECCM technique for radar systems
DATE-ISSUED: May 10, 1994

US-CL-CURRENT: 342/188; 342/159, 342/17, 342/19

INT-CL: [5] G01S 7/36

L13: Entry 8 of 34 File: USPT Apr 27, 1993

US-PAT-NO: 5206826
DOCUMENT-IDENTIFIER: US 5206826 A

TITLE: Floating-point division cell
DATE-ISSUED: April 27, 1993

US-CL-CURRENT: 708/504; 708/650, 708/655

INT-CL: [5] G06F 7/38, G06F 7/52

L13: Entry 9 of 34 File: USPT Jan 26, 1988

US-PAT-NO: 4722069
DOCUMENT-IDENTIFIER: US 4722069 A

TITLE: Nonrestoring divider
DATE-ISSUED: January 26, 1988

US-CL-CURRENT: 708/656

INT-CL: [4] G06F 7/52

L13: Entry 10 of 34 File: USPT Feb 20, 1979

US-PAT-NO: 4141077
DOCUMENT-IDENTIFIER: US 4141077 A

TITLE: Method for dividing two numbers and device for effecting same
DATE-ISSUED: February 20, 1979

US-CL-CURRENT: 708/656

INT-CL: [2] G06F 7/52

L13: Entry 11 of 34 File: USPT Oct 5, 1976

US-PAT-NO: 3983745
DOCUMENT-IDENTIFIER: US 3983745 A

TITLE: Test specimen crack correlator
DATE-ISSUED: October 5, 1976

US-CL-CURRENT: 73/789; 73/799, 73/805, 73/808

INT-CL: [2] G01N 3/36

L13: Entry 12 of 34 File: JPAB Mar 12, 1993

PUB-NO: JP405061649A
TITLE: DIVIDER CIRCUIT
PUBN-DATE: March 12, 1993

INT-CL (IPC): G06F 7/52; G06F 7/00, G06F 9/44

L13: Entry 13 of 34 File: EPAB Feb 2, 1999

PUB-NO: US005867412A
TITLE: Modular multiplication device for information security
PUBN-DATE: February 2, 1999

INT-CL (IPC): G06F 7/38
EUR-CL (EPC): G06F007/72

L13: Entry 14 of 34 File: EPAB Feb 3, 1998

PUB-NO: US005715376A
TITLE: Data transformation apparatus
PUBN-DATE: February 3, 1998

INT-CL (IPC): H04N 1/56
EUR-CL (EPC): G06F017/17 ; H04N001/60

L13: Entry 15 of 34 File: EPAB Apr 8, 1997

PUB-NO: US005619440A
TITLE: Multiplier circuit with rounding-off function
PUBN-DATE: April 8, 1997

INT-CL (IPC): G06F 7/52
EUR-CL (EPC): G06F007/52 ; G06F007/52

L13: Entry 16 of 34 File: EPAB Aug 22, 1995

PUB-NO: US005444647A
TITLE: Multiplier circuit and division circuit with a round-off function

PUBN-DATE: August 22, 1995

INT-CL (IPC): G06F 7/52
EUR-CL (EPC): G06F007/52 ; G06F007/52

L13: Entry 17 of 34 File: EPAB May 10, 1994

PUB-NO: US005311192A
TITLE: Polarization ECCM technique for radar systems
PUBN-DATE: May 10, 1994

INT-CL (IPC): G01S 7/36
EUR-CL (EPC): G01S007/36

L13: Entry 18 of 34 File: EPAB Jun 17, 1993

PUB-NO: DE004141077A1
TITLE: After-waxing installation for sizing unit - comprises slop trough contg. overflow for application substance
PUBN-DATE: June 17, 1993

US-CL-CURRENT: 68/202
INT-CL (IPC): D06B 1/14; D06B 23/24
EUR-CL (EPC): D06B001/14 ; D06B023/24

L13: Entry 19 of 34 File: EPAB Apr 27, 1993

PUB-NO: US005206826A
TITLE: Floating-point division cell
PUBN-DATE: April 27, 1993

INT-CL (IPC): G06F 7/38; G06F 7/52
EUR-CL (EPC): G06F007/52

L13: Entry 20 of 34 File: EPAB Jan 26, 1988

PUB-NO: US004722069A
TITLE: Nonrestoring divider
PUBN-DATE: January 26, 1988

INT-CL (IPC): G06F 7/49
EUR-CL (EPC): G06F007/49 ; G06F007/52
